The following security alert was issued by the Information Security Division of the Mississippi Department of ITS and is intended for State government entities. The information may or may not be applicable to the general public and accordingly, the State does not warrant its use for any specific purposes.

DATE(S) ISSUED:
6/27/2012

SUBJECT:
Multiple Vulnerabilities in Cisco WebEx Recording Format Player Could Allow Remote Code Execution

OVERVIEW:
Multiple vulnerabilities have been discovered in Cisco WebEx WRF (WebEx Recording Format) and ARF (Advanced Recording Format) players, which could allow remote code execution. The WebEx meeting service is a hosted multimedia conferencing solution that is managed and maintained by Cisco WebEx. Sessions established during meetings can be saved to WRF and ARF files and later replayed with Cisco WebEx Players. Successful exploitation of these vulnerabilities could result in either an attacker gaining the same privileges as the logged on user. Depending on the privileges associated with the user, an attacker could install programs; view, change, or delete data; or create new accounts with full user rights.

SYSTEMS AFFECTED:

Cisco WebEx Business Suite Client builds 28.0.0 (T28 L10N)
Cisco WebEx Business Suite Client builds 27.32.1 (T27 LD SP32 CP1) and prior
Cisco WebEx Business Suite Client builds 27.25.10 (T27 LC SP25 EP10) and prior

RISK:
Government:

Large and medium government entities: **High**
Small government entities: **High**

Businesses:

Large and medium business entities: **High**
Small business entities: **High**

Home users: Low

DESCRIPTION:
Multiple buffer overflow vulnerabilities have been discovered in Cisco WebEx (WebEx Recording Format) and ARF (Advanced Recording Format) players that could allow attackers to take user level control of vulnerable system or cause a Denial-of-Service. The Cisco WebEx Recording Format (WRF) player contains four buffer overflow vulnerabilities and the Cisco Advanced Recording Format (ARF) player contains one buffer overflow vulnerability.

The WRF (.wrf) and ARF (.arf) file formats are used to store WebEx meeting recordings that have been recorded on a WebEx meeting site or on the computer of an online meeting attendee. These players can be used to play back and edit recording files using the *.wrf* or *.arf* extensions.

These vulnerabilities may be exploited if a user opens a specially crafted WRF or ARF file. An attacker could accomplish this attack either by an email with an attached malicious recording file to unsuspecting user or by enticing users to visits a maliciously crafted web page.

Successful exploitation could result in an attacker gaining the same privileges of the logged on user. Depending on the privileges associated with the user, an attacker could then install programs; view, change, or delete data; or create new accounts with full user rights.

RECOMMENDATIONS:

The following actions should be taken:

- Upgrade vulnerable Cisco products immediately after appropriate testing.
- Remind users not to visit un-trusted websites or follow links provided by unknown or un-trusted sources.
- Do not open email attachments or click on URLs from unknown or untrusted sources.
- Run all software as a non-privileged user (one without administrative privileges) to diminish the effects of a successful attack.

REFERENCES:

Cisco:

http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20120627-webex
http://support.webex.com/support/support-overview.html

SecurityFocus:

http://www.securityfocus.com/bid/54213

CVE:

http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2012-3053
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2012-3054
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2012-3055
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2012-3056
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2012-3057